AFRL-OSR-VA-TR-2013-0606

SECURE COMMUNICATION VIA KEY GENERATION WITH QUANTUM MEASUREMENT ADVANTAGE IN THE TELECOM BAND

PREM KUMAR

NORTHWESTERN UNIVERSITY - EVANSTON CAMPUS

10/30/2013
Final Report

AIR FORCE RESEARCH LABORATORY
AF OFFICE OF SCIENTIFIC RESEARCH (AFOSR)/RSE
ARLINGTON, VIRGINIA 22203
AIR FORCE MATERIEL COMMAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-09-2013	Final Performance Report	Aug 2009 - Jul 2013

4. TITLE AND SUBTITLE

Secure Communication via Key Generation with Quantum Measurement Advantage in the Telecom Band

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-09-1-0593

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Kumar, Prem
Yuen, Horace
Huang, Yu-Ping

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Northwestern University
633 Clark ST
Evanston, IL 60208

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AF Office of Scientific Research
875 N. Randolph ST. Room 3112
Arlington VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)

AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Quantum Communications, Keyed Communication in Quantum noise, Coherent-state Pulse-Position Modulation, Heralding Sing

14. ABSTRACT

Our goal was to investigate the use of Keyed Communication in Quantum noise as a key generation/distribution mechanism with use of a Coherent-state Pulse-Position Modulation protocol, including designing and constructing in the laboratory proof-of-concept experiments using off-the-shelf telecommunication components, as well as researching security analyses addressing a variety of attack strategies. During this project, on the theoretical front we have completed the investigation of BB84 insecurity. We have shown that trace distance is basically the same guarantee as accessible information and neither is adequate against known-plaintext attacks. On the experimental front we demonstrated an advanced optical modulation format that makes use of both spectral and temporal phase encodings for applications requiring exceptional security. We have successfully used this approach to transmit encrypted 155 Mb/s data over 70 km of fiber with a BER value of 4E-5. In addition, we have performed extensive experimental and theoretical research on independent single-photon sources of high purity, detection of fast quantum optical signals, realization of photonic nonlinearities , and deterministic generation entanglement, etc., all of which could substantially benefit the project goal.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Kumar, Prem
U	U	U	UU	16	**19b. TELEPHONE NUMBER** *(include area code)* 8474912726

Secure Communication via Key Generation with Quantum Measurement Advantage in the Telecom Band

Final Report

(Reporting Period: 1 August 2009 – 31 July 2013)

Sponsored by:

Air Force Office of Scientific Research (AFOSR)

Issued by:

Air Force Office of Scientific Research

Grant # FA9550-09-1-0593

Approved for public release; distribution unlimited

I: Title Page

Name of Grantee: Northwestern University

633 Clark Street, Evanston, IL 60208

Principle Investigator: Prem Kumar

Business Address: Center for Photonic Communication and computing
EECS Departments, Northwestern University
2145 Sheridan Road, Evanston, Illinois 60208-3118

Phone Number: **(**847) 491-4128

Email Address: kumarp@northwestern.edu

Date of Grant: 08/01/2009

Grant Expiration Date: 07/31/2013

II: Summary of Project

In this basic research program we proposed to investigate the use of keyed communication in quantum noise as a key generation/distribution mechanism with use of a coherent-state pulse-position modulation protocol. We proposed to design and construct in the laboratory proof-of-concept experiments using off-the-shelf telecommunications components. We also proposed to research security analyses addressing a variety of attack strategies. Specifically, on the theoretical side, we proposed to (a) investigate using channel coding to alleviate bandwidth requirement for the time-mode realization of the proposed scheme, (b) quantify the behavior of spatial-mode realization for future free-space implementations, and (c) study the possible performance gain by an eavesdropper with other than a universal heterodyne attack. On the experimental side, we proposed to implement quantum limited detection in our running-code OCDMA experiment to demonstrate (a) quantum measurement advantage creation between two users, (b) use of such advantage for key expansion at MHz rates, and (c) use of the expanded key for secure communications through standard optical networking elements.

The major accomplishments we achieved during this project are summarized below.

- Our proposal describes an asymptotic time-spread key generation scheme called CPPM [1] and also a spectral phase encoding scheme which may be considered a finite version of CPPM that is more amenable to experimental implementation. We have theoretically investigated the experimental possibility of implementing such a scheme or using more readily available source and detection technology than those described in the proposal. In particular, we considered the possibility of spreading 100 ps pulses into a thousand slots of 100 ns each, allowing up to 1,000 modes to be used in the CPPM protocol by cutting down the required parameters by three orders of magnitude. We have designed the average coherent-state photon number in each 100 ns, or per time-mode, to be one photon compared to the heterodyne noise level. The total 100 ps signal at 1,000 photons is strong enough to take even considerable loss in the transmission. On the other hand, the signal level per mode is so low that the attacker would not be able to glean much information from a heterodyne attack. The key generation rate before privacy amplification has been quantified. We have determined the key rate reduction when more general attacks are allowed. Note, however, that there is *no* foreseeable technology which would allow Eve to launch an entanglement attack.
- On the theoretical front we have also completed the investigation of BB84 insecurity [2]. We have shown that trace distance is basically the same guarantee as accessible information and neither is adequate against known-plaintext attacks. This is a serious security problem facing the whole field of quantum cryptography in regard to both key generation and direct encryption which is yet to be resolved.
- On the experimental front we proposed and demonstrated an advanced optical modulation format that makes use of both spectral and temporal phase encodings for

applications requiring exceptional security [3]. The method combines modulation techniques used in direct-sequence spread-spectrum coding, spectral-phase encoding, and M-ary phase-shift keying with codes generated using cryptographically secure pseudorandom number generators. The wideband transmission signal is very difficult for an eavesdropper to record or analyze. Signal-to-noise ratio limitations imposed by quantum effects enhance the security further. The properties of the transmitted signal make it especially useful for physics-based key expansion systems. We have successfully used this setup to transmit encrypted 155 Mb/s data over 70 km of fiber with a BER value of 4E-5 [5].

- Using spontaneous optical parametric downconversion, we experimentally demonstrated heralded generation of shaped single photons, whose modes are tailored indirectly by applying amplitude modulation on the pump field that drives the downconversion process [4]. Our experiment opens a door to creating high-quality, mode-shaped single photons at a substantially higher efficiency than is possible with the existing method of direct single-photon shaping.
- We proposed a new avenue towards distillation of quantum entanglement that is implemented by directly passing the entangled qubits through a mode-matched filter. This approach can be applied to a common class of entanglement impurities appearing in photonic systems where the impurities inherently occupy different spatiotemporal modes than the entangled qubits. As a specific application, we show that our method can be used to significantly purify the telecom-band entanglement generated via the Kerr nonlinearity in single-mode fibers where a substantial amount of Raman-scattering noise is concomitantly produced.
- We realized a high rate, ultra-low timing jitter, short optical pulse generator based on cascaded amplitude and phase modulation in an optoelectronic oscillator [8]. The radio-frequency supermodes were shown to be greatly suppressed with the dual-loop architecture, and a highly coherent and flat optical frequency comb was generated. Optical pulses of 12.8 ps duration were obtained with 27.5 fs integrated timing jitter from 100 Hz to 10 MHz.
- We proposed a new methodology, namely, the “quantum Zeno blockade,” for managing light scattering at a few-photon level in general nonlinear-optical media, such as crystals, fibers, silicon microrings, and atomic vapors [9]. Using this tool, antibunched emission of photon pairs can be achieved, leading to potent quantum-optics applications such as deterministic entanglement generation without the need for heralding. In a practical implementation using an on-chip toroidal microcavity immersed in rubidium vapor, we estimated that high-fidelity entangled photons can be produced on-demand at MHz rates or higher, corresponding to an improvement of $\gtrsim 10^7$ times from the state-of-the-art.

- We developed a comprehensive quantum theory for all-optical switches based on nonlinear Sagnac interferometers, where the in-coupling of quantum noise is carefully modeled [10]. When applied to a fiber-loop switch, the theory shows good agreement with the experimental results without using any fitting parameter. This theory can serve as an important guiding tool for configuring switches of this kind for future quantum networking applications.
- We demonstrated in experiment a method applicable to optical systems in which single-mode filtering is used with only linear optical instruments to achieve quantum indistinguishability [11]. Through "heralded" Hong-Ou-Mandel interference experiments we measured and quantified the improvement of indistinguishability between single photons generated via spontaneous four-wave mixing in optical fibers. The experimental results are in excellent agreement with predictions of a quantum-multimode theory we developed for such systems, without the need for any fitting parameter.
- We identified an avenue to realizing optical-nonlinear effects at a single-photon level by exploiting quantum Zeno blockade in nonlinear optical systems [12]. Considering specifically a lithium-niobate microresonator, we found that a deterministic phase gate can be realized between single photons with near-unity fidelity. Supported by established techniques for fabricating and operating such devices, our approach can provide an enabling tool for all-optical applications in both classical and quantum domains.

III: Technical Details of Accomplishments

III. A: A new way to generate fresh secure key: Keyed Communication in Quantum noise

Along this line of research, we studied the possible generation of a fresh key between two users via the process of advantage creation, which is derived from the different ciphertexts or signal observations by the user and an attacker [1]. The quantum key distribution (QKD) protocol of BB84 and its variants are the most well-known examples, although classical scenarios of key generation were available before. There are various problems in utilizing BB84 type protocols in concrete realistic applications, most of which can be traced to the small microscopic signals involved and the need to carry out estimation of the intrusion level for such protocols. We proposed a new approach to QKD via the optimal quantum receiver principle for advantage creation: the structure of a quantum receiver that delivers the optimal performance depends on knowledge of the signal set. We call this new approach [8] KCQ (keyed communication in quantum noise) key generation due to the explicit use of a secret key in the generation process. This KCQ approach does not exist in a classical world in which a single universal observation is optimal for all signal sets. The crucial point of KCQ in contrast to BB84 type QKD protocols is that intrusion level estimation may be omitted as a consequence of the optimal quantum receiver principle, which makes possible among other advantages the use of

strong signals. It is hoped that KCQ would facilitate the adoption of physical key generation methods in practical optical systems. Note that KCQ key generation is in principle totally distinct from the quantum noise randomized direct encryption protocol AlphaEta (αη) or Y-00, which is KCQ direct encryption, although their implementations are closely connected.

Physical cryptography, including KCQ direct encryption as well as BB84 and KCQ key generation, employs secrecy protection mechanisms at the physical signal level away from the bit level at the application layer end of a communication link. It cannot be attacked from such end and Eve has to physically intercept the transmission link with sophisticated technology in order to launch any meaningful attack. This automatically rules out "petty thefts" and constitutes a significant security advantage compared to standard techniques, similar to digital versus analog wireless RF transmissions. Apart from the possibility of rigorous security proofs, which has to be tempered by the corresponding problem of adequate physical modeling, physical cryptography offers a totally new way of securing privacy different from all the standard high-rate cryptographic techniques in use. It is a "new paradigm" in cryptology.

A major implication of our KCQ approach to BB84 type approach is that a pseudo random number generator (PRNG) should be used to generate a running key that determines the users' choice of basis. This should be done even when intrusion level estimation is still employed to retain some BB84 feature for a weak signal or qubit protocol. There are many resulting advantages both from a practical implementation and a theoretical security analysis point of view. The KCQ approach itself seems to hold great promise. Under universal heterodyne attack, we have shown that in principle fresh key generation is quite possible in the CPPM system with respect to the attacker's total probability profile.

III. B: Studies on fundamental quantitative security in quantum key generation

We analyzed the fundamental security significance of the quantitative criteria on the final generated key K in quantum key generation including the quantum criterion *d*, the attacker's mutual information on K, and the statistical distance between her distribution on K and the uniform distribution [2]. For operational significance a criterion has to produce a guarantee on the attacker's probability of correctly estimating some portions of K from her measurement, in particular her maximum probability of identifying the whole K. We distinguished between the raw security of K when the attacker just gets at K before it is used in a cryptographic context and its composition security when the attacker may gain further information during its actual use to help get at K. We compare both of these securities of K to those obtainable from conventional key expansion with a symmetric key cipher. It is pointed out that a common belief in the superior security of a quantum generated K is based on an incorrect interpretation of *d* which cannot be true, and the security significance of *d* is uncertain. Generally, the quantum key distribution key K has no composition security guarantee and its raw security guarantee from concrete protocols is worse than that of conventional ciphers. Furthermore, for both raw and composition security there is an exponential catch-up problem that would make it difficult to quantitatively improve

the security of K in a realistic protocol. Some possible ways to deal with the situation were also suggested.

III. C: Demonstration of running-code optical CDMA at 2 x 10 Gb/s and 40 Gb/s

CDMA has been widely adapted for various radio frequency (RF) communication applications. Recently, CDMA has been in the research arena of optical communications and is referred to as optical CDMA (OCDMA). OCDMA can provide an inherent physical layer security and is also capable of various networking functions, including code translation, which may make it a suitable candidate for use in future advanced optical networks. Owing to the high bit rates in optical communications, encoding has often been performed in polarization and/or frequency domains. In contrast to the temporal coding in RF CDMA, which results in spread spectrum characteristics, spectrum encoding will cause temporal spreading leading to temporal overlap and obscuration of neighboring bits. The effect of the spectral phase encoding resembles an extreme case of chromatic dispersion except with an unnatural spectral phase profile. Present spectral coding methods typically use static phase masks from which each of the users is assigned one mask pattern. The phase masks do not need to be changed on fast time scales allowing technologies such as liquid crystal array or thermally tuned ring resonator based encoders to be viable. Although the static code can provide a certain level of security, the longer a particular code is used the more time and signal-to-noise ratio an eavesdropper has to attack it. To fully utilize the OCDMA technology from a security perspective, ideally one would update the code sequence at the bit rate, but such a system is prohibitively expensive to implement with current technology. We developed an OCDMA system with a running-code spectral phase mask which substantially enhances the security level of the spectral phase coding OCDMA scheme by placing a time limit on an attacker's attempt to measure or exhaustively search for the mask. Differential phase shift keying (DPSK) is also incorporated in our system as the preferred modulation method, eliminating simple intensity analysis being possible as is the case with on-off keyed OCDMA systems.

III. D: Experimental demonstration of lossless single-photon shaping via heralding

Pure single photons are a prerequisite for many applications in quantum information processing (QIP), ranging from quantum cryptography to linear optical quantum computing. To achieve optimal performance, such photons are required to be prepared in appropriate spatiotemporal modes. For example, in cavity QED quantum communication, single photons in the waveform of temporally symmetric pulses are generally employed to minimize cavity-coupling losses. Quantum-state transfer between light and matter waves, in contrast, is most efficient for photons in rising exponential pulses. For QIP applications based on interference effects, single photons in Gaussian waveforms are superior, whereas for differential-phase-shift quantum key distribution, single photons in coherent pulse trains are required. To prepare single

photons in appropriate spatiotemporal modes, the existing method is to apply direct phase or amplitude modulation on the created single-photon pulses. However, because the devices used for creating these modulations usually involve significant transmission losses, such a method substantially reduces the production efficiency of the shaped photons. This drawback cannot be simply overcome by increasing the mean photon number per pulse, because doing so degrades the quality of the shaped single photons due to increased multiphoton production. Therefore, the direct shaping method is overly restrictive for practical QIP.

To overcome the modulation loss and thereby greatly improving the production efficiency of shaped single photons, we analyzed and experimentally demonstrated an indirect single-photon shaping technique implemented via "heralding" [4]. Heralding is a quasi-on-demand method to create single photons, in which a photon (idler photon) in a photon pair is detected in order to predict the presence of the other photon of the pair (signal photon). Using such a method, high-purity single photons have been generated with high efficiency in both $\chi^{(2)}$ crystals and $\chi^{(3)}$ optical fibers. In our indirect shaping technique, the spatiotemporal modes of the heralded signal photons are tailored indirectly by (i) modulating the pump mode that creates the photon pairs and (ii) appropriately measuring the idler photons. As no direct modulation of any kind is applied on the heralded photons, the modulation loss is eliminated. As a result, the production efficiency of mode-shaped single photons can be substantially higher than that obtainable via direct modulations on the single photons that have already been created. Our technique can be generally applied to heralded single-photon generation in any system that employs a parametric nonlinear optical process.

III. E: Experiment on two-dimensional optical code-division modulation with quantum-noise aided encryption for applications in key distribution

We moved toward an enhanced security regime for quantum communications allowed by a multidimensional encoding scheme consisting of simultaneous incorporation of spectral-phase encoding (SPE) running code, a fast binary time-mode code, and an AlphaEta M-ary phase code. All the codes are generated from PRNGs based on the advanced encrypted standard (AES). A 10 GHz pulse train is modulated with a differential phase-shift keyed (DPSK) 155 Mb/s data sequence together with an AlphaEta pseudorandom 4096-ary phase shift to strongly encrypt the transmission. Thus, there are 64 mode-locked pulses in each data symbol such that each pulse can contain a small number of photons, while the entire data symbol has a proportionally larger number of photons. Each pulse is also modulated using a pseudo-randomly chosen binary time-mode phase code, and the resulting pulse sequence is dispersed in time by a dynamically varying SPE code such that the pulse train strongly overlaps in the time domain. The spectral-phase code has up to 40 spectral-phase bins applied via an acousto-optic modulator (AOM) whose evolving phase mask is fully updated approximately every 2 microseconds.

III. F: Proposed new method for distilling quantum entanglement via mode-matched filtering

Quantum entanglement is an essential resource for a variety of potent applications that are unparalleled by classical means, such as quantum synchronization, sensing, dense coding, cryptography, computing, and teleportation. The performance of these applications depends critically on the purity of the entanglement resources they have access to. Inevitably in practice, the entanglement is generated and distributed with impurities due to in-coupling of background noises. In photonic systems, these noises arise, for example, from imperfect optical operations, transmission through noisy channels, or more fundamentally, from spontaneous emission of uncorrelated photons. In order to obtain highly pure entanglement, a procedure called "entanglement distillation (or purification)" must be applied to separate the quantum entanglement from the noises. Several ancillary entanglement distillation protocols have been proposed, including the so-called one-way hashing protocol, two-way recurrence protocol, and their variations. These protocols are probabilistic in nature and consume a considerable amount of ancillary entangled qubits. They also require local operations and classical communication (LOCC), including single-qubit measurements. Hence, the efficiency and speed of implementing such protocols are low and overly restricted.

Furthermore, when applied to photonic entanglement, quantum memories may be required. We proposed a different avenue towards entanglement distillation that is realized directly via mode-matched filtering. Our approach can deal with a class of impurities resulting from quantum noises that are produced by different physical processes than that creating the entangled qubits. Noises of this kind exist quite commonly in practice. For example, in atomic-vapor sources of entangled photon pairs, spontaneous background photons are emitted via non-phase-matched processes. Such photons are thus in different temporal modes than the entangled photons which are generated via coherent, phase-matched, two-photon super-radiant emission. Similarly, in optical fibers the background Raman photons produced through the retarded molecular response are in different temporal modes than the entangled photons generated predominantly through the instantaneous electronic response. Our idea of direct entanglement distillation (DED) is to construct a mode-matched filter that only passes the spatiotemporal modes of the entangled qubits while rejecting the other modes containing noise. For photonic qubits, such a filter can be built from a sequence of devices operating in the spectral and temporal domains. Passing through such a filter, the quantum entanglement can be distilled directly from the noises without the use of ancillary entanglement resources or LOCC. Our approach thus has the potential to substantially improve the efficiency and speed of entanglement distillation.

III. G: Proposed new methods for distilling quantum entanglement via mode-matched filtering

High rate, ultra-stable short optical pulses are desired for high resolution analog to digital converters (ADCs) and optical samplers, which are key components in a variety of applications in microwave photonics, communications, and instrumentation. The low jitter and narrow durations possible with optical pulse sources are critical for achieving high ADC resolution and bandwidth. We have demonstrated a 10 GHz rate, ultra-stable short optical pulse source using cascaded amplitude and phase modulation in a dual-loop opto-electronic oscillator (OEO) [8]. Trains of optical pulses with 12.8 ps pulse width and 27.5 fs integrated timing jitter from 100 Hz to 10 MHz are generated. The design uses the same fiber spool to act as a low-loss delay element in one of the feedback loops and to simultaneously compress the generated pulses. The obtained narrow pulse width and the low timing jitter are ideal characteristics of this source for photonic ADC and other jitter-sensitive applications.

III. H: Proposal for deterministic nonlinear-optical sources of entangled photons

Generation of quantum entanglement is an interdisciplinary, long-lasting effort, triggered more than 50 years ago by Bell's quantum non-locality argument in response to the hidden-variable theory of Einstein, Podolsky, and Rosen. Motivated by the fundamental tests of quantum uncertainty in earlier days, the quest for efficient sources of entanglement nowadays has been fueled by a variety of potent applications that are otherwise unrealizable by classical means. For most of these applications, entanglement embodied in pairs of photons has been recognized as an ideal resource owing to its robustness against decoherence, the convenience of its manipulation with linear-optical components, as well as the ease of distribution over long distances at the speed of light. Thus far, entangled photon pairs have mostly been generated probabilistically via post-selection, where the quantum-entanglement features are established only after selecting favorable measurement outcomes. While such photon pairs are useful for some proof-of-principle demonstrations of quantum effects, practical applications beyond a few-qubit level will require on-demand sources of entangled photons.

The obstacle to deterministic generation of entangled photons in nonlinear-optical media arises fundamentally from the stochastic nature of the photon-pair emission process, because of the inherent quantum randomness in how many photon pairs will be created in a given time interval. To overcome this randomness, existing methods have relied on ‘‘heralding’’ schemes in which auxiliary photons are detected in order to project a multi-photon-pair state onto an entangled single-pair state. In these schemes, however, a fourfold coincidence measurement or a twofold coincidence measurement after nonlinear-optical mixing must be adopted. Because such operations are extremely inefficient, the production rate of entangled photons is fundamentally restricted to the sub-Hertz range.

In this project, we proposed and demonstrated via simulation a new methodology for managing light scattering in general nonlinear media, which allows us to directly overcome (i.e., without the use of heralding) the stochastic nature of the photon-pair emission process [9]. The idea is to employ novel ‘‘quantum Zeno blockade’’ (QZB), which suppresses the creation of multiple photon pairs in a single spatiotemporal mode through the quantum Zeno effect, while the creation of a single pair is allowed. It is achieved by coupling the photon-pair system to a dissipative reservoir in a way that the coupling is efficient only when more than one pair of photons is present. When the coupling is sufficiently strong, the creation of multiple photon pairs is then blocked (suppressed) through the quantum Zeno effect. As a result, the photon pairs are created in a pairwise ‘‘antibunching’’ manner similar to that of antibunched emission of single photons by a single atom. Such effect can lead to deterministic generation of entangled photons at MHz rates or higher by using existing technology. Note that while QZB relies on strong coupling between multiple pairs of photons and a reservoir, but when it is in effect, ideally no energy dissipation or quantum-state decoherence will actually occur as the creation of multiple pairs will be inhibited.

III. I: Experiment on single-mode filtering

We investigated a pathway to erasing quantum distinguishability by making use of the Heisenberg uncertainty principle [11]. This method, although designed specifically for optical systems, might be generalizable to other physical systems, including those of atoms and ions. It uses a filtering device that consists of only linear optical instruments, which in our present rendering is a temporal gate followed by a spectral filter. The gate’s duration T and the filter’s bandwidth B (in angular hertz) are chosen to satisfy $BT < 1$ so that any photon passing through the device loses its temporal (spectral) identity as required by the Heisenberg uncertainty principle. In this sense, the device behaves as a singlemode filter (SMF) that passes only a single electromagnetic mode of certain temporal profile while rejecting all other modes. Hence, applying such a SMF to distinguishable single photons can produce output photons that are indistinguishable from each other. We note that the general principle underlying the use of a SMF is known, and similar methods have been applied in various experiments. However, a systematic, quantitative analysis has yet to be performed. Here we present such a systematic study of the SMF method, both theoretically and experimentally, considering specifically a fiber-optical system. In theory, we developed a comprehensive quantum multimode model of light scattering and detection in optical-fiber systems, taking into account multi-pair emission, Raman scattering, transmission loss, dark counts, and other practical parameters. Our simulations using this model showed that for appropriate parameters very high levels of quantum indistinguishability can be achieved with use of the SMF, while paying a relatively low cost in terms of photon loss. In contrast, using tight spectral or temporal filtering alone for similar purposes results in much higher photon loss.

In experiment, we measured in two different regimes of operation Hong-Ou-Mandel (HOM) interference between single photons that are generated separately from two sources via heralding [11]. Specifically, pairs of signal and idler photons were generated in two separate optical-fiber spools via spontaneous four-wave mixing. By detecting the idler photons created in each spool, we heralded the generation of their partner (signal) photons. To quantify their indistinguishability, we mixed the signal photons generated separately from the two spools on a 50:50 beam splitter and performed HOM interference measurements. We found that the HOM visibility is quite low when the signal photons have a temporal length $T > 1/B$, owing to the presence of photons with many distinguishable degrees of freedom. However, when $T < 1/B$, a SMF is effectively realized and a much higher HOM visibility was obtained. This result clearly showed that the SMF can be used to erase the quantum distinguishability of single photons. The experimental data are in good agreement with predictions of the multimode model without the need for any fitting parameter.

III. J: Theory development of photonic nonlinearity via quantum Zeno blockade

The quest for information processing by all-optical means has fueled new studies of optical phenomena in an extreme quantum regime involving only a few photons. This requires optical nonlinearities that are orders of magnitude higher than those achievable with existing optical media. Although this drawback can be overcome by combining strong cavity enhancement with resonant coupling between photons and (effective) atoms, the implementation requires large setups and operation in near-zero-temperature environment, making such systems unsuitable for practical use. In contrast, schemes based on post-selection or feed-forward can be implemented with only linear-optics instruments. Such schemes, however, are inherently probabilistic in their outcomes and thus their use is hard to justify in large-scale applications. Highly off-resonant optical nonlinearities, on the other hand, do not suffer from the aforementioned issues and are thus potentially viable for photonic information processing tasks on a large scale. It was suggested that intense cross-phase modulation (XPM) in Kerr-nonlinear media could produce a deterministic phase gate between single photons. This idea, unfortunately, was developed upon an incorrect single-mode argument. By taking into account the inherent multimode nature of light propagation in a Kerr medium, it was recently discovered that no useful XPM effect can be produced in such systems even with an unrealistically giant Kerr nonlinearity. The fundamental reason turns out to be that causality prohibits XPM phase shift of any non-negligible amount without significant quantum noise. It remains an outstanding challenge—not only because of implementation difficulties but also due to the fundamental restrictions—to construct practical nonlinear optical devices suitable for operation at the single photon level.

We proposed to surmount this challenge by exploiting the quantum Zeno effect that occurs when a slowly evolving system is probed frequently, or continuously, with the result that the system is “frozen” in its initial state (i.e., its evolution is slowed down) [12]. Applying this

effect to a nonlinear optical cavity, quantum Zeno blockade (QZB) can be realized whereby occupation of a cavity mode "blocks" (more precisely, suppresses) additional photons from entering the cavity. In effect, the intracavity photon acts as a continuous probe monitoring the in-coupling of additional photons, thereby preventing them from entering the cavity through the Zeno effect. QZB is analogous in functionality to "photon blockade" that is realized through vacuum Rabi splitting. QZB instead occurs through the Zeno effect, which allows for distinct "interaction-free" operations that can potentially lead to ultralow-loss and noise-free devices for all-optical processing. We employed QZB to realize strong, interaction-free nonlinear effects between single photons. Specifically, by considering a second-order nonlinear system of a prism-coupled lithium niobate (LN) microdisk resonator, we show that strong XPM effects can be produced between single photons under realizable parameter settings. When the input single photons are in the form of Gaussian pulses, they become entangled at the output. However, when the input photons are prepared in exponential waveforms that are time reversed replicas of the cavity leakage modes, a deterministic phase gate can be realized. This result highlights a potentially enabling pathway for implementing practical photonic information processing. Our approach is generally extendable to a variety of nonlinear optical systems of traveling-wave or resonator designs.

IV: Conclusion and Outlook

During the course of this program, we have investigated, both experimentally and theoretically, the use of Keyed Communication in Quantum noise as a key generation/distribution mechanism with use of a Coherent-state Pulse-Position Modulation protocol. We designed and constructed in the laboratory proof-of-concept experiments using off-the-shelf telecommunication components. We also researched security analyses addressing a variety of attack strategies. In addition, we have made significant progress in generating, routing, detecting, and interacting quantum optical signals, including single and entangled photons. These progresses together can potentially lead to realization of robust quantum communications in a practical industrial setting.

Through this research, we have seen that realistic QKD generated keys have inadequate raw security and no composition security guarantee. One may obtain much better raw security probability guarantee with conventional ciphers. The perception to the contrary is due mainly to a mistaken interpretation of a security criterion which has actually no clear operational security significance. On the other hand, physical cryptography, including KCQ direct encryption as well as BB84 and KCQ key generation, employs secrecy protection mechanisms at the physical signal level away from the bit level at the application layer end of a communication link. It cannot be attacked from such end and Eve has to physically intercept the transmission link with sophisticated technology in order to launch any meaningful attack. This automatically rules out "petty thefts" and constitutes a significant security advantage compared to standard techniques,

similar to digital versus analog wireless RF transmissions. Apart from the possibility of rigorous security proofs, which has to be tempered by the corresponding problem of adequate physical modeling, physical cryptography offers a totally new way of securing privacy different from all the standard high-rate cryptographic techniques in use. It is a "new paradigm" in cryptology.

A major implication of our KCQ approach to BB84-type approach is that a PRNG should be used to generate a running key that determines the users' choice of basis. This should be done even when intrusion-level estimation is still employed to retain some BB84 feature for a weak signal or qubit protocol. There are many resulting advantages both from a practical implementation and a theoretical security analysis point of view. The KCQ approach itself seems to hold great promise. Under universal heterodyne attack, we have shown that in principle fresh key generation is quite possible in the CPPM system with respect to the attacker's total probability profile. Finally, it is well to recall that we still need to develop a meaningful and sufficiently strong security measure that can be usefully estimated and achieved in concrete realistic protocols.

V. List of Publications

V. A: Journal Papers:

[1] H. P. Yuen, "Key Generation, Foundation and a New Quantum Approach," IEEE J. Selected Topics in Quantum Electronics, Vol. 15, 1630-1645 (2009).

[2] H. P. Yuen, "Fundamental Quantitative Security in Quantum Key Generation," Phys. Rev. A, Vol. 82, 062304 (2010); arXiv:1008.0623v2.

[3] S. X. Wang, D. R. Reilly, G. S. Kanter, S. Ozharar, and P. Kumar, "Running-code optical CDMA at 2 x 10 Gbit/s and 40 Gbit/s," IEE Electronics Letters, Vol. 46, 701–703 (2010).

[4] K. G. Köprülü, Y.-P. Huang, G. A. Barbosa, and P. Kumar, "Lossless single-photon shaping via heralding," Optics Letters, Vol. 36, No. 9, May 1, 2011, pp. 1674–1676.

[5] S. Ozharar, D. R. Reilly, S. X. Wang, G. S. Kanter, and P. Kumar, "Two-dimensional optical code-division modulation with quantum-noise aided encryption for applications in key distribution," J. Lightwave Technology, Vol. 29, No. 14, 15 July 2011, pp. 2081–2088; Digital Object Identifier (DOI): 10.1109/JLT.2011.2156760.

[6] Y.-P. Huang and P. Kumar, "Distilling quantum entanglement via mode-matched filtering," Physical Review A, Vol. 84, No. 3, 032315(5) 13 September 2011. See also http://arxiv.org/abs/1108.4699, 23 August 2011.

[7] Y.-P. Huang, J. B. Altepeter, and P. Kumar, "Optimized heralding schemes for single photons," Physical Review A, Vol. 84, No. 3, 033844(7) 20 September 2011; http://dx.doi.org/10.1103/PhysRevA.84.033844.

[8] J. Liu, G. S. Kanter, S. Wang, and P. Kumar, "10 GHz ultra-stable short optical pulse generation via phase-modulation enhanced dual-loop optoelectronic oscillator," Optics Communications, Vol. 285, No. 6, pp. 1035–1038, 30 November 2011; doi:10.1016/j.optcom.2011.11.053.

[9] Y.-P. Huang and P. Kumar, "Antibunched Emission of Photon Pairs via Quantum Zeno Blockade," Physical Review Letters, Vol. 108, No. 3, 030502(5), 20 January 2012; http://dx.doi.org/10.1103/PhysRevLett.108.030502

[10] Y.-P. Huang and P. Kumar, "Quantum theory of all-optical switching in nonlinear Sagnac interferometers," New Journal of Physics Vol. 14 No. 5, 053038 (14) 25 May 2012; http://dx.doi.org/10.1088/1367-2630/14/5/053038

[11] M. Patel, J. B. Altepeter, Y.-P. Huang, N. N. Oza, and P. Kumar, "Erasing Quantum Distinguishability via Single-Mode Filtering," Physical Review A, Vol. 86, No. 3, 033809 (5) 6 September 2012; http://dx.doi.org/10.1103/PhysRevA.86.033809

[12] Y.-Z. Sun, Y.-P. Huang, and P. Kumar, "Photonic Nonlinearities via Quantum Zeno Blockade," Physical Review Letters, Vol. 110, No. 22, 223901(5), 31 May 2013; http://dx.doi.org/10.1103/PhysRevLett.110.223901

V. B: Articles in Hard-Bound Volumes:

K. T. McCusker, Y.-P. Huang, A. S. Kowligy, D. V. Strekalov, Y.-Z. Sun, and P. Kumar, "All-Optical Switching via the Quantum Zeno Effect," in Proceedings of the 10th Rochester Conference on Coherence and Quantum Optics (CQO-X) and the 2nd Conference on Quantum Information and Measurement (QIM-2) (The Optical Society, Washington, DC).

V. C: Conference Papers:

Y.-P. Huang, K. G. Köprülü, G. A. Barbosa, and P. Kumar, "Lossless single photon shaping via heralding," presented at the Conference on Nonlinear Optics 2011, Marriott Kauai Beach Resort, Kauai, HI, July 17–22, 2011; paper NMB6. See NLO'2011 Technical Digest (The Optical Society, Washington, D.C., 2011).